(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
25 août 2005 (25.08.2005)

PCT

(10) Numéro de publication internationale
WO 2005/079090 A1

(51) Classification internationale des brevets[7] : H04Q 7/32, 7/38

(21) Numéro de la demande internationale :
PCT/FR2005/000328

(22) Date de dépôt international :
11 février 2005 (11.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0401347 11 février 2004 (11.02.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

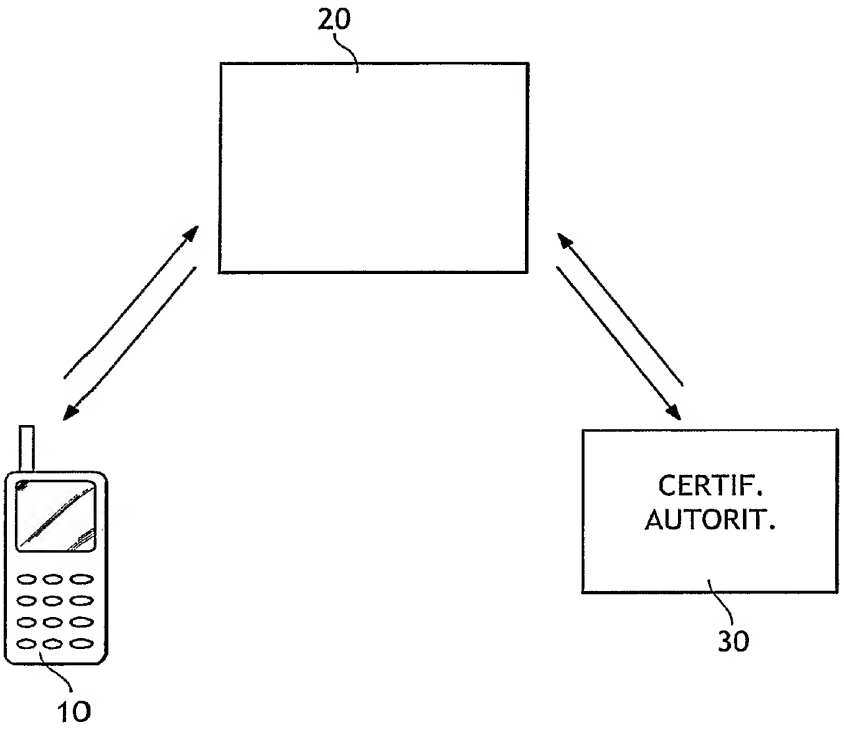
(75) Inventeurs/Déposants *(pour US seulement)* : **ARDITTI, David** [FR/FR]; 46ter, rue Paul Vaillant Couturier, F-92140 Clamart (FR). **LABBE, Bruno** [FR/FR]; 13, rue Gustave Courbet, F-78370 Plaisir (FR). **BEGAY, Didier** [FR/FR]; Villeneuve, F-16430 Champniers (FR).

(74) Mandataires : **JOLY, Jean-Jacques** etc.; Cabinet Beau de Loménie, 158, rue de l'Université, F-75340 Paris Cedex 07 (FR).

[Suite sur la page suivante]

(54) Title: EMISSION OF A PUBLIC KEY BY A MOBILE TERMINAL

(54) Titre : EMISSION DE CLE PUBLIQUE PAR UN TERMINAL MOBILE



30 ... CERTIF. AUTHORITY

(57) Abstract: The invention relates to a method of certification involving a public key certification authority (30) and at least one mobile terminal (10) which can receive messages which are encrypted by said public key, characterized in that it comprises a stage which consists in generating the public key in the mobile terminal (10), a stage wherein a telecommunications network entity (20) acquires said key from the terminal (10) by means of a network communication, and a stage wherein the terminal (10) is authenticated for the network entity by means of an authentication process of the interlocutor used in a conventional telephone communication, said method comprising a stage wherein the public key is supplied to the certification authority (30) along with the result of the identification process.

[Suite sur la page suivante]

WO 2005/079090 A1

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de certification faisant appel à une autorité de certification (30) de clé publique et faisant appel à au moins un terminal mobile (10) apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape consistant à générer la clé publique au sein du terminal mobile (10) lui-même, l'étape consistant, pour une entité (20) de réseau de télécommunications à acquérir cette clé auprès du terminal (10) par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal (10) par un processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification (30) cette clé publique en association avec le résultat de ce processus d'identification.

EMISSION DE CLE PUBLIQUE PAR UN TERMINAL MOBILE

L'invention concerne une infrastructure à clé publique dans un réseau de téléphonie mobile.

L'invention concerne également les terminaux informatiques mobiles, possédant notamment une carte SIM ou WIM.

De tels terminaux peuvent donc être des téléphones mobiles ou des téléphones WAP.

Ils présentent en commun la caractéristique d'avoir une carte SIM ou WIM donc d'être déjà identifié sur un réseau en rapport de l'opérateur auquel le service de téléphonie mobile a été souscrit.

Plus spécifiquement, l'invention concerne notamment une infrastructure à clé publique dans un réseau mobile.

Une question universelle et récurrente dans le domaine des réseaux est comment assurer la confiance entre interlocuteurs qui ne se connaissent pas et à distance. La solution existe, elle consiste à mettre en œuvre une infrastructure à clé publique (ICP ou PKI, Public Key Infrastructure).

Cette infrastructure possède l'avantage d'offrir aux intervenants utilisant cette infrastructure de s'appuyer sur une couche de sécurité élevée permettant l'authentification forte, la signature et le chiffrement. En revanche, elle présente l'inconvénient de son organisation qui reste complexe, longue, difficile à mettre en place et donc onéreuse pour un opérateur.

De nos jours, les interactions entre les différentes entités identifiées par les certificats et l'autorité de certification sont une part importante de la gestion des certificats, c'est à dire des approbations incluant, à titre essentiel, une clé publique. Ces interactions incluent des opérations telles que l'enregistrement pour la certification, le renouvellement de certificat, la révocation de certificat, la sauvegarde et le recouvrement des clés. En général, une CA (Certification Authority) doit être capable d'authentifier les identités des entités avant de répondre aux demandes. En plus les

demandes ont besoin d'être approuvées par des administrateurs autorisés ou des gestionnaires avant d'être mises en service.

Les moyens utilisés par les différentes Autorités de Certification pour vérifier une identité avant de délivrer un certificat peuvent varier largement. Cela dépend notamment de l'organisation et de l'usage du certificat.

Pour se procurer plus de souplesse, les interactions avec les utilisateurs peuvent être séparées des autres fonctions de l'Autorité de Certification et gérées par un service à part appelé autorité d'enregistrement (Registration Authority ou RA).

Une RA agit comme une interface entre la CA en recevant les demandes des utilisateurs, les authentifiant, et les transmettant à la CA. Après réception de la réponse de la CA, la RA notifie à l'utilisateur le résultat. Les RA peuvent être utiles à l'échelle d'une PKI à travers les différents départements, sur des zones géographiques différentes ou toutes autres unités dont la politique et les demandes d'authentification varient.

On peut noter ici les inconvénients de cette infrastructure : elle est longue et coûteuse à mettre en place, elle possède peu de souplesse dans la génération des certificats (liés à la politique de certification), elle a un coût important pour l'usager qui désire posséder un certificat, elle nécessite une gestion importante du côté de l'opérateur de certification.

En d'autres termes, une infrastructure à clé publique offre une sécurité élevée, mais présente l'inconvénient d'une inscription préalable auprès d'une autorité d'enregistrement.

L'invention vise à rendre plus aisé le processus de certification de clé publique.

Ce but est atteint selon l'invention grâce à un procédé de certification faisant appel à une autorité de certification de clé publique et faisant appel à au moins un terminal mobile apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape consistant à générer la clé publique au sein du terminal mobile lui-même, l'étape consistant, pour une entité de réseau de télécommunications, à acquérir cette clé auprès du terminal par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal par un

processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification cette clé publique en association avec le résultat de ce processus d'identification.

Un tel procédé permet notamment à un abonné à un réseau mobile, la génération d'une bi-clé par exemple puis la délivrance d'un certificat par l'opérateur.

On propose également selon l'invention un système de télécommunications mobiles, comprenant au moins un terminal mobile et une entité de réseau, caractérisé en ce qu'il comporte des moyens pour générer une clé publique au sein du terminal mobile lui-même et des moyens au sein de l'entité de réseau de télécommunications pour acquérir cette clé publique auprès du terminal par une communication de réseau, ainsi que des moyens d'authentification du terminal par un processus d'authentification utilisé dans une communication téléphonique habituelle, le système comprenant en outre une autorité de certification et des moyens pour fournir à l'autorité de certification la clé publique générée par le terminal mobile en association avec le résultat de ce processus d'authentification.

On propose en outre un terminal de télécommunication mobile, caractérisé en ce qu'il inclut des moyens de production d'au moins une clé destinée à déchiffrer des messages reçus par ce terminal, ainsi que des moyens pour émettre cette clé par une communication de réseau via une entité de réseau de téléphonie, à destination d'une autorité de certification de sorte que celle-ci devienne une clé publique.

D'autres caractéristiques, buts et avantages de l'invention apparaîtront à la lecture de la description détaillée qui va suivre, faite en référence à la figure unique annexée, qui représente une infrastructure de certification conforme à une variante préférée de l' invention.

L'idée ici est de générer la bi-clé (clé publique et clé privée) sur le mobile de l'utilisateur puis de transmettre la clé publique à une autorité de certification par l'intermédiaire du réseau de téléphonie mobile à l'aide d'un canal sécurisé.

Cette solution décentralise les démarches et reporte la délivrance de la bi-clé dans le mobile. Cette solution allège la phase de délivrance/authentification de certificat et a un coût nul pour l'usager. Pour l'opérateur, les éléments constituant cette infrastructure sont allégés.

Cette idée permet en outre de déplacer la phase d'enregistrement, cette phase étant alors aisément réalisée au moment de la souscription d'un abonnement au service de téléphonie mobile.

Elle offre l'avantage donc de pratiquement s'affranchir de cette phase.

On introduira d'abord les éléments spécifiques à l'administration actuelle des clés et des certificats. L'ensemble des moyens qui permettent l'utilisation des clés publiques et des certificats à des formats normalisés dans un environnement réseau est généralement appelé Public Key Infrastructure (PKI).

L'administration d'une PKI est un sujet complexe (gestion des clés, des certificats, listes de révocation, recouvrement...).

Le procédé de délivrance des certificats dépend de l'autorité de certification dont ils sont issus et de leur usage. La délivrance d'un certificat doit s'effectuer selon une procédure bien définie et si l'on veut que ce certificat ait une valeur, en « face à face » après, par exemple, examen de papiers d'identité.

Différentes autorités de confiance élaborent différentes politiques de délivrance de certificats.

Dans certains cas, seule l'adresse électronique suffit.

Dans d'autres cas, le login UNIX ou Windows et un mot de passe sera suffisant.

A l'opposé, pour des certificats disposant de prérogatives importantes, le procédé de délivrance peut requérir au préalable des documents notariaux, ou encore une vérification complète de l'identité en « face à face ».

Selon la politique d'organisation, le procédé de délivrance des certificats peut prendre une forme complètement transparente pour

l'utilisateur (au détriment de la sécurité) ou demander la participation significative de l'utilisateur et des procédures complexes.

En général ces procédés de délivrance de certificats doivent être très souples, ainsi les organisations peuvent les adapter à leur besoin.

Avant qu'un certificat soit délivré, la clé publique qu'il contient doit être générée en correspondance d'une clé privée qui, elle, est confidentielle.

Quelquefois, il peut être utile de délivrer un certificat à une personne pour des opérations de signature et un autre certificat pour une utilisation de chiffrement.

Les clés privées, qu'elles soient de signature ou de chiffrement, sont gardées sur un support physique (carte à puces, d'ongle, USB, ...), support physique qui est détenu par la personne qu'il représente, pour assurer une sécurité élevée.

Dans un objectif de recouvrement, la clé privée de chiffrement est séquestrée sur un serveur central protégé où elle pourra être retrouvée dans le cas où l'utilisateur perd sa clé par exemple.

Une clé de chiffrement spécifiquement dédiée aux communications téléphoniques est généralement produite soit en local (poste de travail ou même à l'intérieur d'une carte à puce) ou de façon centrale par exemple dans un atelier de personnalisation de carte à puce.

Par exemple, la génération de clés en local assure un service maximum de non répudiation, mais implique plus de participation de l'utilisateur dans le procédé de délivrance. La souplesse de gestion des clés est essentielle pour la plupart des organisations sans négliger le côté sécurité.

Comme une carte d'identité, un certificat est soumis à une période de validité. Toute tentative d'utilisation d'un certificat avant ou après sa période de validité échouera.

Donc les mécanismes pour l'administration et le renouvellement de certificats sont essentiels pour la politique de sécurité.

Un administrateur peut vouloir être averti quand un certificat expire, ainsi un procédé de renouvellement approprié peut être mis en place et

éviter tout désagrément quant à l'utilisation de certificats qui arrivent à expiration. Le procédé de renouvellement de certificat peut impliquer la réutilisation de la même paire clé publique/clé privée ou la délivrance d'une autre.

Un certificat peut être suspendu même s'il est en cours de validité, lors d'un vol par exemple.

De manière similaire, il est quelquefois nécessaire de révoquer un certificat avant sa date d'expiration. Par exemple, si un employé quitte son entreprise ou se fait voler le support de sa bi-clé.

La révocation de certificats consiste à publier une liste de révocation de certificats (Certificate Revocation List, CRL) dans un annuaire à intervalles réguliers. La vérification de cette liste fait alors partie intégrante du procédé d'authentification.

On décrira maintenant les éléments qui se trouvent habituellement mis en œuvre de manière à assurer l'identification d'un interlocuteur et la sécurité de la communication concernée, au sein d'un réseau de télécommunications, et qui sont, pour certains de ceux ci-après décrits, mis en œuvre dans le cadre de la présente variante de l'invention.

L'infrastructure d'un réseau mobile a été conçue de manière à garantir une sécurité élevée. Le système GSM a donc recours à des procédés d'authentification et de chiffrement. Afin de garantir ce niveau de sécurité élevée, le réseau authentifie le mobile de manière forte.

Le système GSM utilise quatre types d'adressage lié à l'abonné :

- l'IMSI n'est connu qu'à l'intérieur du réseau GSM ;
- le TMSI correspond à une identité temporaire utilisée pour identifier le mobile lors des interactions mobile/réseau ;
- le MSISDN correspond au numéro de téléphone de l'abonné, c'est le seul identifiant connu de l'extérieur.
- le MSRN, qui est un numéro attribué lors de l'établissement de l'appel.

Après avoir rappelé les différentes dispositions de type communes dans les réseaux de communications téléphoniques, nous allons définir maintenant quelques acronymes.

L'abréviation SIM (Suscriber Identifiant Module) définit un module d'identifiant de l'abonné.

L'abréviation IMSI (International Mobile Station Identity) qualifie un identifiant unique de l'abonné (15 chiffres), stocké dans la carte SIM.

L'abréviation TMSI (Temporary Mobile Suscriber Identity) qualifie une identité propre à un VLR, identité temporaire de l'abonné dans le VLR.

L'abréviation MSISDN (Mobile Station International ISDN Number) qualifie, elle, une identité de l'abonné qui est visible dans le monde téléphonique (exp : 33 6 98 76 54 32).

Le IMEI (International Mobile Equipement Identity) est l'identité du terminal.

Le MSRN (Mobile Station Roaming Number) est l'identité nécessaire pour acheminer les appels entre le MSC passerelle vers le PSTN et le MSC courant du mobile.

Afin d'éviter toute utilisation d'un compte mobile par une personne autre que l'abonné 10, le système GSM a recours à un procédé d'authentification visant à protéger à la fois l'abonné mais aussi l'opérateur.

Un abonné 10 désirant s'authentifier sur le réseau, le réseau via une entité de communication 20, transmet alors un nombre aléatoire appelé RAND au mobile. La carte SIM calcule la signature de RAND à l'aide de l'algorithme A3 et la clé privée Ki stockée dans la carte SIM.

Le résultat obtenu est noté SRES, puis envoyé au réseau.

Le réseau (ici l'entité 20), pour s'assurer de l'identité de cet abonné, va faire de même, c'est à dire qu'il calcule une signature de RAND à l'aide de A3 et de la clé Ki propre à chaque abonné et stocké sur une base de données.

Si le résultat calculé en local est identique à celui réceptionné, l'abonné est authentifié, dans le cas contraire le mobile est rejeté.

Pour réaliser cette confidentialité, on va générer ici une clé de chiffrement appelée Kc. Cette clé se construit à l'aide de la donnée aléatoire transmise par le réseau et d'une clé privée Ki propre à l'abonné 10 et stockée dans la carte SIM.

Avec ces deux paramètres une clé Kc est générée avec l'aide de l'algorithme A8. De son côté, le réseau (l'entité 20) réalise la même opération.

La clé Ki correspondant à l'abonné identifié précédemment se trouve dans une base AUC (Authentification Center), et le réseau obtient avec cette clé Ki la même clé de chiffrement Kc de son côté.

L'idée est de définir un modèle de PKI allégée avec ici les objectifs suivants, qui sont ceux de diminuer le coût de gestion pour l'opérateur, c'est à dire éviter une architecture lourde et centralisée et de s'appuyer sur la sécurité de l'architecture de téléphonie et en particulier sur l'identification/authentification sur laquelle repose le système.

Il est à noter que cette solution peut s'adresser à des échanges sécurisés comme par exemple dans un environnement de travail afin de préserver la confidentialité des échanges ou bien dans le cadre de communications en peer-to-peer.

Comme on l'a vu précédemment, la procédure d'authentification possède des éléments de sécurité élevée. Une fois cette phase (authentification/confidentialité) terminée, l'idée est de générer dans le téléphone un bi-clé.

Par la suite, l'abonné 10 envoie sa clé publique à un opérateur de certification (ici l'entité 20 elle-même). Le rôle d'opérateur de certification est donc au moins tenu partiellement par l'opérateur de téléphonie mobile lui-même.

L'authentification sur le réseau GSM est de ce fait une authentification forte (possession d'un élément de sécurité et d'un secret).

Cet envoi au serveur de certification 30 est réalisé dans un tunnel sécurisé.

En d'autres termes, après réception de la clé publique, l'opérateur 20 peut certifier cette clé réceptionnée, car il est certain de l'identité correspondante à la clé publique présentée : non usurpation de l'identité possible sur le réseau GSM. Puis l'opérateur 20 renvoie le certificat à son propriétaire (cas où l'entité 20 et confondue avec l'autorité de certification) et/ou le dépose sur le serveur publique de certification, ici référencé 30.

Les avantages de cette solution sont énormes, notamment la procédure de certification simplifiée, l'absence ici de processus de recouvrement, et une gestion décentralisée et reportée sur le client.

L'idée est donc de générer ici la bi-clé au sein du mobile 10 avec ici les principes selon lesquels le DN (distinguished name, ou identifiant unique) pour chaque possesseur de certificat est son numéro de téléphone et chaque possesseur de certificat génère sa bi-clé et obtient un certificat par envoi de sa clé publique pour certification de manière traditionnelle. Le serveur détermine automatiquement à l'aide du DN l'origine de l'appel.

En outre, l'authentification de l'expéditeur (l'abonné 10) est réalisée par le réseau de téléphonie (l'entité 20). L'entité de certification 30 qui génère le certificat en correspondance avec la clé reçue est certaine de l'identité certifiée dans le certificat, grâce à l'action d'identification réalisée par l'entité de téléphonie 20, et ses moyens d'identification habituels de terminal mobile.

Le serveur 30 peut donc enfin générer le certificat correspondant à la clé publique reçu puis envoyer le certificat à son propriétaire.

Le procédé décrit est mis en œuvre par un programme d'ordinateur.

Ce programme d'ordinateur est destiné à être stocké dans / ou transmis pas un support de données, et comporte des instructions logicielles pour faire exécuter le procédé par un dispositif informatique, en l'espèce, le dispositif de mesure décrit.

REVENDICATIONS

1. Procédé de certification faisant appel à une autorité de certification (30) de clé publique et faisant appel à au moins un terminal mobile (10) apte à recevoir des messages qui soient chiffrés par cette clé publique, caractérisé en ce qu'il comporte l'étape consistant à générer la clé publique au sein du terminal mobile (10) lui-même, l'étape consistant, pour une entité (20) de réseau de télécommunications, à acquérir cette clé auprès du terminal (10) par une communication de réseau, et l'étape consistant, pour l'entité de réseau, à authentifier le terminal (10) par un processus d'authentification de l'interlocuteur utilisé dans une communication téléphonique habituelle, le procédé comprenant en outre l'étape consistant à fournir à l'autorité de certification (30) cette clé publique en association avec le résultat de ce processus d'authentification.

2. Procédé selon la revendication 1, caractérisé en ce que l'étape d'authentification du mobile (10) inclut l'émission par le mobile (10) d'un résultat de calcul faisant intervenir une clé confidentielle stockée dans le mobile, et l'étape de comparaison, par l'entité de réseau (20), du résultat avec un résultat attendu, calculé également par l'entité de réseau (20) à partir de cette même clé confidentielle, une comparaison positive étant interprétée comme une identification du terminal mobile.

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend l'étape consistant, pour l'entité de réseau, à émettre à l'attention du terminal, une donnée aléatoire, l'étape de calcul par le terminal faisant intervenir également cette donnée aléatoire émise par l'entité de réseau, l'étape de calcul par l'entité de réseau faisant aussi intervenir cette donnée aléatoire en vue de ladite comparaison de résultat.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il met en œuvre l'étape consistant à générer au sein même du terminal mobile (10), outre la clé publique, une clé confidentielle gardée en mémoire dans le mobile (10) et adaptée à déchiffrer des messages reçus et qui ont été chiffrés avec la clé publique.

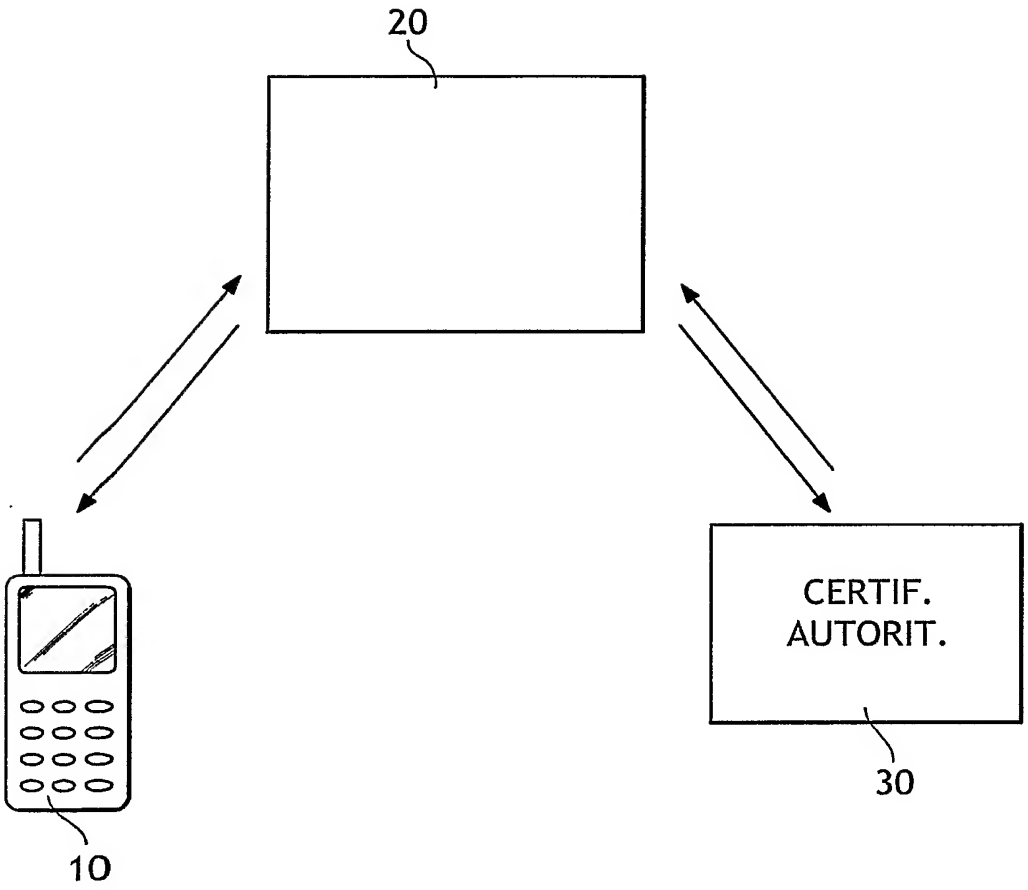
5. Procédé selon la revendication 4, caractérisé en ce que le terminal est prévu pour émettre des messages et y apposer une signature d'authentification produite à l'aide de la clé confidentielle générée par lui-même précédemment.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'étape consistant, pour l'entité de réseau (20), à envoyer la clé publique à l'autorité de certification (30) via un canal qui est sécurisé contre des lectures non autorisées.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'étape consistant pour le mobile (10) à utiliser une clé d'authentification de ce mobile (10) utilisée habituellement dans ses communications téléphoniques et à générer une clé de chiffrement, puis à chiffrer des messages à l'aide de cette clé de chiffrement puis à émettre de tels messages.

8. Système de télécommunications mobiles, comprenant au moins un terminal mobile (10) et une entité de réseau (20), caractérisé en ce qu'il comporte des moyens pour générer une clé publique au sein du terminal mobile (10) lui-même et des moyens au sein de l'entité de réseau de télécommunications (20) pour acquérir cette clé publique auprès du terminal (10) par une communication de réseau, ainsi que des moyens d'authentification du terminal par un processus d'authentification utilisé dans une communication téléphonique habituelle, le système comprenant en outre une autorité de certification et des moyens pour fournir à l'autorité de certification la clé publique générée par le terminal mobile en association avec le résultat de ce processus d'authentification.

9. Terminal de télécommunication mobile (10), caractérisé en ce qu'il inclut des moyens de production d'au moins une clé destinée à déchiffrer des messages reçus par ce terminal, ainsi que des moyens pour émettre cette clé par une communication de réseau via une entité de réseau de téléphonie (20), à destination d'une autorité de certification (30) de sorte que celle-ci devienne une clé publique.


20
CERTIF.
AUTORIT.
30
10

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2005/000328

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/32 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/210789 A1 (FARNHAM ET AL.) 13 November 2003 (2003-11-13) page 3, paragraphs 31,32 page 4, paragraph 33 figure 2	1-9
Y	MENEZES A J; OORSCHOT VAN P C; VANSTONE S A: "Handbook of Applied Cryptography, BLOCK CIPHERS" 1997, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US , XP002299647 page 559 - page 560	1-9

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June 2005	21/06/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	M. García

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2005/000328

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003210789 A1	13-11-2003	GB 2384403 A	23-07-2003
		CN 1507720 A	23-06-2004
		WO 03061190 A1	24-07-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2005/000328

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04Q7/32 H04Q7/38

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 2003/210789 A1 (FARNHAM ET AL.) 13 novembre 2003 (2003-11-13) page 3, alinéas 31,32 page 4, alinéa 33 figure 2	1-9
Y	MENEZES A J; OORSCHOT VAN P C; VANSTONE S A: "Handbook of Applied Cryptography, BLOCK CIPHERS" 1997, HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US , XP002299647 page 559 - page 560	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 juin 2005	21/06/2005

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	M. García

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/FR2005/000328

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003210789 A1	13-11-2003	GB 2384403 A	23-07-2003
		CN 1507720 A	23-06-2004
		WO 03061190 A1	24-07-2003